AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

LISTING OF CLAIMS:

Claims 1 to 7. (Canceled).

8. (Currently Amended) A method for implementing an encryption system, comprising the steps of:

generating a Vernam key via a symmetrical cipher, the generating being aided by using a secret key and a variable parameter, the Vernam key having a length that is equal to a length of a message to be protected, the secret key having a defined key length, the variable parameter having a length which is a function of the defined key length;

encrypting, via a Vernam key, the message using logic operations of a Vernam cipher;

communicating, from a sending point to a receiving point, the secret key and the variable parameter via at least one of (A) a secure channel separate from a message-transmission path and (B) the message-transmission path, the message-transmission path being secured via an asymmetrical cipher;

regenerating the Vernam key; ~~and~~

decrypting the message using the regenerated Vernam key;

installing a storage space and one of a symmetrical cipher and the asymmetrical cipher in a crypto-module, the crypto-module being separate from an encryptor; and

performing encryption operations via the Vernam cipher in the encryptor.

9. (Previously Presented) The method according to claim 8, wherein the encryption system uses a Vernam cipher.

10. (Previously Presented) The method according to claim 9, wherein the Vernam cipher is a very simple mathematical operation.

11. (Previously Presented) The method according to claim 10, wherein the very simple mathematical operation is EXOR.

12. (Currently Amended) The method according to claim 8, further comprising:

~~installing a symmetrical cipher and a storage space in a crypto-module, the storage space~~ storing the Vernam key in the storage space~~, the crypto-module being separate from an encryptor, the encryptor including at least one of a chip card, a multifunctional PC interface adapter and a PCMCIA module~~; and

performing Vernam cipher operations exclusively in the encryptor, wherein the encryptor includes ~~including~~ at least one of a chip card, a multifunctional PC interface adapter and a PCMCIA module.

13. (Currently Amended) The method according to claim 8, ~~further comprising the steps of:~~ wherein the crypto-module is

~~implementing the asymmetrical cipher and a storage space in~~ an external crypto-module; and further comprising~~, the external crypto-module being separate from the encryptor; and~~

controlling, via the Vernam cipher, encryption operations in the encryptor.

14. (Currently Amended) The method according to claim 8, wherein the Vernam key is stored in ~~an~~ the encryptor.

15. (Previously Presented) An encryption system, comprising:

means for generating a Vernam key via a symmetrical cipher, the generating being aided by using a secret key and a variable parameter, the Vernam key having a length that is equal to a length of a message to be protected, the secret key having a defined key length, the variable parameter having a length which is a function of the defined key length;

means for encrypting, via a Vernam key, the message using logic operations of a Vernam cipher;

means for communicating, from a sending point to a receiving point, the secret key and the variable parameter via at least one of (A) a secure channel separate from a message-transmission path and (B) the message-transmission path, the message-transmission path being secured via an asymmetrical cipher;

means for regenerating the Vernam key;

means for decrypting the message using the regenerated Vernam key;

crypto-hardware including at least one of a chipcard and a multifunctional PC interface adapter with built-in special crypto-hardware; and

the encryptor being capable of coupling to the crypto-hardware, the encryptor including at least one of a personal computer, software and a terminal which implements a Vernam cipher for broad-band applications in software.

16. (Previously Presented) The encryption system according to claim 15, wherein the crypto-hardware is designed as an external crypto-module and wherein the crypto-hardware has an intermediate storage, the intermediate storage storing reserve storage of the Vernam key.

17. (Previously Presented) The encryption system according to claim 16, wherein the intermediate storage is disposed in one of the personal computer and the terminal.

18. (Currently Amended) An encryption system, comprising:

a secret key having a defined key length;

a variable parameter having a length which is a function of the defined key length;

a symmetrical cipher;

a Vernam key having a length that is equal to a length of a message to be protected; the Vernam key being generating via the symmetrical cipher with aid from the secret key and the variable parameter, the Vernam key encrypting the message using logic operations from a Vernam cipher; ~~and~~

at least one of a message-transmission path and a secure channel, the message-transmission path being a path over which the encrypted message is communicated, the message-transmission path being secured via an asymmetrical cipher, the secure channel being separate from the message-transmission path; and

a crypto-module including a storage space and one of the symmetrical cipher and the asymmetrical cipher, wherein the crypto-module is separate from the encryptor, the storage space is used to store the Vernam key, and any Vernam cipher operations are performed in the encryptor,

wherein the secret key and the variable parameter are communicated over at least one of the message-transmission path and the secure channel and, subsequently, used in regenerating the Vernam key, the regenerated Vernam key decrypting the message.